BR DATA security

SOLUÇÕES

AMBIENTE SEGURO – SEUS NEGÓCIOS DEPENDEM DISSO!

O ambiente de Tecnologia da Informação (TI) vem se tornando cada vez mais complexo, qualquer alteração ou configuração incorreta pode torná-lo vulnerável à exposição de informações sigilosas e à perda da integridade e disponibilidade de sistemas corporativos.

ANÁLISE DE RISCOS

Cada vez mais as organizações, seus sistemas de informação e redes de computadores são colocados à prova por diversos tipos de ameaças, incluindo vazamento de informações, fraudes, roubos e invasões (físicas e lógicas). Problemas causados por vírus e hackers são freqüentes e proliferam a cada dia.

A Análise de Riscos tem por objetivo mapear as ameaças e vulnerabilidades do ambiente de negócios.

O que é

Consiste em um processo de identificação dos riscos de segurança que o negócio está exposto. É realizada através de uma avaliação sistemática que visa o mapeamento das ameaças e vulnerabilidades nos ativos de tecnologia, processos, pessoas e ambiente físico.

Objetivo

Diagnosticar a situação da Segurança da Informação na organização e recomendar ações (contramedidas) para cada vulnerabilidade mapeada

Metodologia

Os projetos realizados pela **BR Data Security** são desenvolvidos de acordo com a Metodologia de Análise de Riscos de Segurança (M.A.R.S) que constitui todos os nossos produtos. Nossa metodologia é fundamentada na BS7799 que deu origem a ISO/IEC 17799 – Norma de Segurança da Informação reconhecida mundialmente como melhores práticas para a Gestão da Segurança da Informação.

Benchmarking

Para uma perfeita avaliação da situação da organização em relação a Segurança da Informação, é realizado um estudo comparativo com outras organizações. Este comparativo conhecido como Benchmarking tem como objetivo mostrar o grau de segurança que pode determinar vantagem comparativa. Quesitos considerados na média e/ou abaixo dos níveis mercadológicos podem ser revistos para obtenção de padrão de segurança adequado.

Resultado

É apresentado em relatório personalizado informando o atendimento atual da organização quanto as melhores práticas para a gestão da segurança da informação e as recomendações para a implementação de medidas preventivas conforme as necessidades da organização. Todas as recomendações são discutidas com o cliente, para que ele receba a melhor orientação possível e tenha maior facilidade em tomar decisões com base nas informações levantadas.

Apresentação Executiva dos Resultados

Apresentação Executiva dos resultados da Análise de Riscos em slides, direcionada ao grupo executivo sumarizando os resultados obtidos com enfoque estratégico.

Produtos Finais

- Workshop com a equipe do projeto
- Relatório de Análise de Riscos
- Resumo Executivo
- Matriz de Criticidade
- Plano de Ação de curto, médio e longo prazo
- Apresentação Executiva dos resultados

Componentes da Análise de Riscos

- Entrevistas com gestores para avaliação dos processos críticos e impactos aos negócios
- Entrevistas com usuários para avaliar seu comprometimento quanto à segurança das informações
- Relatório de nível estratégico
- Relatório de nível tático
- Relatório de nível operacional
- Apresentação Executiva dos resultados
- Reunião de follow-up após o término do projeto

.: ANÁLISE DE RISCOS MODULAR

Você determina o escopo da Análise de Riscos, podendo iniciar o trabalho em ambientes específicos e ampliar progressivamente o foco da análise para outros setores da empresa, incorporando aos poucos a segurança na cultura da organização.

Benefícios

- Conhecimento da real situação da empresa
- Identificação das medidas de segurança apropriadas
- Orientação para formalização das regras de segurança
- Definição dos níveis de serviço para Segurança da Informação
- Conhecimento das potenciais ameaças ao ambiente de negócios
- Aderência a padrões internacionais de segurança (ISO/IEC 17799)

Compreendendo a Segurança da Informação no dia-a-dia

- Negação de serviço (problemas de DISPONIBILIDADE)
- Destruição de ativos (problemas de DISPONIBILIDADE)
- Modificação não autorizada do conteúdo de seu Website (problemas de INTEGRIDADE)
- Vazamento de informações (problemas de CONFIDENCIALIDADE)

O exemplo acima mostra como os componentes de negócio dependem dos ativos, caso estes sofram danos, também ocorre um impacto no negócio.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação serve como base ao estabelecimento de normas e procedimentos que garantem a segurança da informação, bem como determina as responsabilidades relativas à segurança dentro da empresa.

A elaboração de uma Política de Segurança da Informação deve ser o ponto de partida para o gerenciamento dos riscos associados aos sistemas de informação.

Para atender as principais necessidades da empresa, uma Política de Segurança da Informação deve ser:

- clara e concisa
- de fácil compreensão
- coerente com as ações da empresa
- amplamente divulgada
- revisada periodicamente

Descrição do Serviço

A Política de Segurança da Informação visa preservar a confidencialidade, integridade e disponibilidade das informações. Descrevendo a conduta adequada para o seu manuseio, controle, proteção e descarte.

Sua empresa possui uma Política de Segurança da Informação? Se, sim oferecemos o serviço de análise e revisão da sua política, visando a aderência à ISO 17799.

Produtos Finais

- Carta do Presidente
- Diretrizes de Segurança da Informação
- Normas de segurança
- Exemplo de Procedimentos Operacionais
- Exemplo de Instruções Técnicas
- Termo de Sigilo e Responsabilidade

Benefícios

- Comprometimento da alta direção, com a continuidade dos negócios
- Aumento da conscientização da empresa quanto a segurança das informações
- Padronização nos processos organizacionais
- Definição das responsabilidades pelos ativos da empresa
- Conformidade com a Legislação e obrigações contratuais

TESTE DE INVASÃO

O Teste de Invasão é uma ferramenta eficiente, que possibilita validar ou encontrar novas falhas na segurança do ambiente. Tem como principal objetivo identificar brechas de segurança e penetrar nos sistemas da empresa, visa também sensibilizar o cliente dos riscos que seu ambiente está exposto.

Pesquisas indicam que a maioria dos ataques são feitos por funcionários ou seja, são realizados por pessoas de dentro da própria empresa.

Descrição do serviço

A análise do ambiente corporativo sob a perspectiva do chamado hacker ético, permite que sejam identificadas potenciais vulnerabilidades que a empresa apresenta ao mundo externo e interno.

São feitas simulações de ataques, com as mesmas técnicas e ferramentas utilizadas pelos invasores. Todo o processo do Teste de Invasão é controlado.

O Teste de Invasão pode ser divido em diferentes abordagens: tentativa de intrusão tecnológica interna e/ou externa e tentativa de intrusão processual (engenharia social, análise do lixo corporativo e etc).

Para que este serviço possa ser realizado faz-se necessário a assinatura de um **TERMO DE CONFIDENCIALIDADE** entre as partes.

Benefícios

- Conhecimento das vulnerabilidades que sua empresa está exposta
- Determinar prioridades quanto à Segurança da Informação
- Subsídio para que decisões estratégicas sejam tomadas com fatos reais

IMPLEMENTAÇÃO DE SEGURANÇA

Com o aumento no número de ameaças internas e externas, as empresas passaram a exigir maiores controles para reduzirem os riscos em relação às perdas potenciais se as falhas de segurança ocorrerem.

Identificadas as ameaças e os riscos, é preciso selecionar e implementar os controles necessários para assegurar que os riscos sejam reduzidos a um nível de segurança aceitável.

A Implementação de Segurança realizada pela **BR Data Security** leva em consideração a melhor relação custo/benefício para sua empresa.

Descrição do Serviço

Este serviço tem por objetivo corrigir falhas de segurança através da configuração de controles no ambiente tecnológico.

Benefícios

- Controles implementados conforme as necessidades de cada ativo
- Garantia da confidencialidade, integridade e a disponibilidade das informações

CAMPANHA DE DIVULGAÇÃO

A melhor forma de conquistar o usuário como aliado em um processo de gestão de segurança da informação é tornando-o consciente de suas responsabilidades e dos riscos que enfrentará em seu dia a dia.

Uma empresa que possui uma área de engenharia, o engenheiro deve estar ciente da possibilidade de vazamento ou corrupção da informação; a área comercial da mesma forma, preocupada com a confidencialidade, disponibilidade, integridade e privacidade da informação, e nas conseqüências que este comprometimento pode acarretar.

A conscientização de segurança deve ser vista como auxiliar indispensável aos controles tecnológicos planejados ou já implementados. A cultura organizacional pode trazer grandes benefícios para a organização; o principal deles sem dúvida alguma é o comprometimento.

Um usuário comprometido é um grande aliado, tanto na utilização segura da informação, quanto no mapeamento de riscos ainda não identificados. Quanto maior for o conhecimento deste usuário, maior será sua capacidade de julgamento, refletindo em uma postura proativa, madura e coerente frente às suas responsabilidades no processo de segurança.

Ao invés de perceber a segurança como um adicional à sua atividade, o usuário deverá reconhecer a segurança como parte da sua atividade.

Objetivo

Atividade com o propósito de disseminar a cultura de segurança, sensibilizar e apresentar melhores práticas para a utilização dos recursos de informação da organização. A Campanha de Divulgação é realizada a partir dos dados colhidos por nossa equipe junto ao cliente.

Produtos Finais

- Palestras
- Plano de Ação
- Folhetos
- Mousepad
- Cartilha

Benefícios

- Divulgação dos conceitos de segurança aplicado às rotinas de trabalho
- Melhor aceitação de novos controles de segurança
- Conscientização sobre os riscos que a empresa está exposta

MONITORAMENTO E GERENCIAMENTO DE SEGURANÇA

Manter uma infra-estrutura de segurança atualizada e operacional não é uma tarefa fácil para a maioria das empresas.

O **Monitoramento e Gerenciamento de Segurança (MGS)** é um conjunto de serviços permanentes que tem como objetivo manter a infra-estrutura de TI da sua empresa com níveis elevados de segurança.

Ao contratar este serviço sua empresa terá acompanhamento contínuo da segurança do ambiente operacional. Conheça os serviços que compõem o **MGS**:

1) ANÁLISE DE VULNERABILIDADES

Novas vulnerabilidades surgem a cada dia e uma infra-estrutura de segurança desatualizada pode comprometer a continuidade de seus negócios. A Análise de Vulnerabilidades tem como objetivo mapear todas as vulnerabilidades existentes no ambiente de tecnologia. O cliente recebe mensalmente um relatório contendo as informações sobre as vulnerabilidades encontradas, as recomendações para cada vulnerabilidade e a evolução do ambiente analisado.

2) CORREÇÃO DE VULNERABILIDADES

A maior parte das invasões ocorrem através da exploração de vulnerabilidades antigas e conhecidas. A Correção de Vulnerabilidades tem como objetivo eliminar as vulnerabilidades identificadas durante a análise de segurança. Porém, as medidas e os controles a serem implementados só serão executados com a anuência do cliente.

3) ALERTAS DE SEGURANÇA

Diariamente são descobertas e reportadas novas vulnerabilidades nos diversos sistemas de processamento de dados existentes. O serviço de Alertas de Segurança tem como objetivo alertá-lo sobre as novas vulnerabilidades que podem afetar os servidores de sua empresa.

4) SUPORTE DE SEGURANÇA

Com o surgimento de novas tecnologias, vulnerabilidades e ameaças, as organizações precisam garantir a disponibilidade dos recursos de informação que dão suporte ao negócio. O Suporte de Segurança fornece atendimento local ou remoto à empresa, buscando a solução dos problemas de segurança e a manutenção preventiva do ambiente operacional. A execução deste serviço leva em conta a severidade do problema e retorno com prazo definido.

5) GERÊNCIA REMOTA

Com a crescente onda de incidentes de segurança, as empresas cada vez mais precisam garantir que seus mecanismos de proteção estão configurados adequadamente. A Gerência Remota permite que modificações sejam executadas remotamente e que as configurações de segurança de seus sistemas estarão de acordo com as necessidades de cada ativo.

6) ATUALIZAÇÃO DE PRODUTOS

Quanto mais complexa se torna sua infra-estrutura de segurança, maior é o desafio para mantê-la atualizada. A Atualização de Produtos visa manter seu ambiente de segurança com as últimas correções disponibilizadas por cada fornecedor.

7) RESPOSTA A INCIDENTES DE SEGURANÇA

Uma infra-estrutura segura reduz os riscos de ataques e minimiza os danos que podem ser causados. Entretanto, é impossível garantir que todos os ataques serão evitados. A Resposta a Incidentes de Segurança fornece suporte emergencial para assegurar uma resposta rápida, ordenada e efetiva aos incidentes de segurança caso estes ocorram.

Benefícios

- Equipe do cliente focada em seu Core Business
- Redução de custo e complexidade da administração de segurança

.: OBJETIVOS DA SEGURANÇA DA INFORMAÇÃO

1. Manter a confiança dos clientes, parceiros, acionistas e contribuintes na organização;
2. Proteger a confidencialidade, integridade e disponibilidade de informações sensíveis;
3. Proteger as informações operacionais contra leitura não autorizada;
4. Evitar responsabilizações por ações ilegais ou maliciosas cometidas através dos sistemas da organização;
5. Garantir que os computadores, a rede e os dados da organização não sejam desperdiçados ou abusados;
6. Evitar fraudes;
7. Evitar acidentes custosos ou que causem interrupção dos negócios;
8. Estar de acordo com leis e regulamentações;
9. Evitar um ambiente de trabalho hostil.

Fonte: GAO/AIMD 98-68

SEPS 705/905 Bloco "A" Sala 206 – Centro Empresarial Santa Cruz – Asa Sul – Brasília (DF) – CEP 70390-055
Para maiores informações envie e-mail para info@brdatanet.com.br